## REMARKS

IDS ACKNOWLEDGEMENT

The Examiner lined through document B2 cited in the FORM PTO 1449 of the IDS of December 31, 2008. It is understood that according to the USPTO IFW the copy of the cited document B2 was not legible, so another copy of the document B2 is submitted in an IDS. Consideration and acknowledgement of the document B2 is requested.

REJECTIONS

Claims 6, 8-21 and 23-31 are pending.

The independent claim is 10.

35 USC 112, second paragraph, and 35 USC 101 Rejection:

Claims 6, 8-21 and 23-31 are rejected under 35 USC 112, second paragraph, and 35 USC 101 for indefiniteness and for being directed to non-statutory subject matter by allegedly being hybrid claims that overlap two different statutory classes of inventions under 35 USC 101. The indefiniteness rejection is traversed, because the language of claim 10 clearly requires "A computer system for conducting an agreement between two parties relying on a ***Secure Transaction Server*** as a trusted third party ~~server~~ comprising: ***a first party consumer mobile device*** comprising a computer processor that executes ... and ***a second party merchant device*** comprising a computer processor that executes ... wherein ~~only~~ the STS exclusively stores the personal identifying information of the first party as the second input mobile device parameter." It is readily apparent that the claimed ***computer system*** includes a ***first party consumer mobile device*** and ***a second party merchant device***, which include computer processors that execute the recited operations. In addition, the Secure Transaction Sever is a machine that "~~only~~ stores exclusively the personal identifying information of the first party as the second input mobile device parameter," so the language of claim 10 does not recite a method of using the Secure Transaction Server, but clearly recites what the Secure Transaction Server does. In other words, reliance upon MPEP 2173.05(p) cannot be appropriate, because it is readily apparent that the language of claim 10 is directed to a computer system that executes the recited inventive operations as functional limitations, such that the computer system is transformed into a new computer system in relation to prior art computer systems. In view of MPEP 2173.05(g), the language of the claims do not overlap two different statutory classes of

invention under 35 USC 101, but the operations are functional limitations defining what the devices do rather than by what the devices are.

In addition, the language of claim 10 is amended to improve form.

For the reasons discussed above, withdrawal of the 35 USC 112, second paragraph, and 35 USC 101 rejections is requested.

35 USC 112, first paragraph, rejection:

Claims 6, 8-21 and 23-31 are rejected under 35 USC 112, first paragraph, for failing to comply with the written description requirement.

The Office Action Response to Arguments page 2 provides that paragraph 487 and FIG. 31 do not show the "first view" or "second view" and these sections do not show deriving a key. In addition, the Response to Arguments page 2 provides the specification does not express the relationship that FIG. 31's consumer message is "a first view of the agreement" and merchant message is "a second view of the agreement."

Regarding the claim language 'first view of the agreement ..., a second view of the agreement ...' for example, FIGs. 29-31 expressly illustrate the consumer message as the first view of the agreement and a merchant message as the second view of the agreement. For example, paragraph 178 expressly discusses 'the UPTD 102 generates its own view of the transaction ... The MTS 104 also computes its own view of the transaction.' In FIG. 1, the UPTD 102 is the claimed "mobile device" and the merchant transaction server (MTS) 104 is the claimed "merchant device." It is also readily apparent that paragraph 208 supports the claims. Further, paragraph 250 expressly ties FIGs. 29-31 consumer and merchant messages to the language of claim 10's "a first view of the agreement ... and ... a second view of the agreement" by describing:

> The consumer device 102 generates and transmits a consumer message (ConsumerMsg) including a plaintext part ($DID_C$ and Time Stamp of the consumer device) and an encrypted part (***Transaction view of the consumer***, consumer user ID ($UID_C$), and merchant device ID ($DID_M$).

Similarly, paragraph 254 describes:

> The encrypted part of the merchant message is generated by the merchant device 104 as follows. The merchant device 104 encrypts the merchant's PIN ($PIN_M$) and the merchant's Random Sequence Number ($RSN_M$), using encoding functions (algorithms) of the Secure Agreement Submission protocol (or STP) discussed

> herein below with reference to Figures 57-63, to form the merchant KEY ($KEY_M$). The merchant device 104 then encrypts (again using the encoding functions (algorithms) discussed herein below with reference to Figures 57-63 ***the merchant's view of the Transaction***, merchant user ID ($UID_M$), and consumer device ID ($DID_C$) using the merchant key, to generate the encrypted part of the merchant message.

Similarly, paragraphs 251 and 260 describe:

> Referring again to Figure 29, the consumer device 102 generates the encrypted part of the consumer message as follows. ***The consumer device 102 encrypts the consumer's PIN ($PIN_C$) and the consumer's Random Sequence Number ($RSN_C$), using encoding functions (algorithms) of the Secure Agreement Submission protocol (or STP) discussed herein below with reference to Figures 57-63, to form the consumer KEY ($KEY_C$)***. The consumer device 102 then encrypts (again using the encoding functions (algorithms) discussed herein below with reference to Figures 57-63 the Transaction, consumer user ID, and merchant device ID using the consumer key, to generate the encrypted part of the consumer message.
>
> Figures 31 and 32 show generating, transmitting, and decoding a consumer message and a merchant message using the consumer device ID ($DID_C$) in place of the consumer user ID ($UID_C$), and the merchant device ID ($DID_M$) in place of the merchant user ID ($UID_M$). ***As in the case of Figures 29 and 30***, the ***Transaction views of the consumer and the merchant included, respectively, in the consumer message and the merchant message***, are compared directly with each other by the STS 106 to determine if they match. However, in Figures 31 and 32, the consumer's device id ($DID_C$s) included in the consumer message and in the merchant message are compared directly with each other by the STS 106 to determine if they match, and the merchant's device id ($DID_M$) included in the consumer message and in the merchant message are compared directly with each other by the STS 106 to determine if they match.

For example, from these descriptions, it is readily apparent that the specification does express the relationship that FIGs. 29-31 consumer message is "a first view of the agreement" and merchant message is "a second view of the agreement." Withdrawal of the 35 USC 112, first paragraph, rejection in connection with the first and second views of claim 10 is requested.

In addition, regarding the key generation, paragraphs 487, 534-535 and FIG. 58 expressly support the claims, namely support "generating a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement pertaining to ordering and/or purchasing goods and/or services, ~~and~~ securing the first view of the

agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device." Paragraph 487 provides:

> ***The key derivation algorithm combines information about the mobile computing device with information about the user of the device. The algorithm also combines information that is stored digitally by the device and the shared secret information that is input by the user.*** Such a combination ensures with high likelihood that only the intended parties are able to decrypt and thus access the communicated data. If a device is lost or stolen, it can not be used without the specific user input information, which itself is not stored on the device. The deterministic key derivation algorithm may be generally known. The set of stored parameters is preferably known only to the device and the verification party, but if generally known are not sufficient to determine the key, without knowledge of the shared secret value. The secret value, or the stored parameters, or the key are never transmitted in a message. ***What is transmitted is a message parts of which are encrypted with a key that is derived from the stored parameters and the shared secret information that is input by the user.***

In other words, an aspect of an embodiment of the invention is directed to the parameters utilized for the key derivation, namely "***securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***." Paragraphs 487 and 534-535 and FIG. 58 literally or expressly describe the claimed 'key derivation' and comply with 35 USC 112, first paragraph.

In addition, FIGs. 29-31 illustrate to one skilled in the art the claimed key derivation, for example, by showing in the consumer message the $Key_c$ generated based upon the $RSN_c$, (i.e., the consumer mobile device's Random Sequence Number as the "first mobile device parameter") and $PIN_c$ (i.e., as "input personal identifying information ... as a second input mobile device parameter"). According to an aspect of one embodiment, the $RSN_c$ is generated or derived from a device unique parameter of an original seed, for example, a device identifier (DID) (in a non-limiting example see FIG. 58 and paragraphs 534-535). Withdrawal of the 35 USC 112, first paragraph, rejection in connection with the claimed key derivation is requested.

Obviousness-type Double Patenting Rejection:

Claim 10 is rejected on the ground of non-statutory obviousness-type double patenting over US Patent No. 7,349,871. The Office Action asserts that related US Patent No. 7,349,871 discloses all the features of claim 10 except the concept of using a key to secure the view, and that since the claims of the patent and the present invention performs a similar function, it would have been obvious to modify the present invention by removing the additional element resulting essentially in the same invention. The Office Action also provides 'Thus, omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.' However, the language of independent claim 10 requires other patentably distinguishing features and claim 10 is amended by requiring "***generating ... a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement ..., securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***."

The Office Action does not provide an obviousness analysis between all required limitations in the language of claim 10 and the language of claim 1 of US Patent No. 7,349,871.

In addition, claim 10 as amended is patentably distinguishing from claim 1 of US Patent No. 7,349,871, rendering moot the obviousness double patenting rejection. Withdrawal of the obviousness double patenting rejection is requested.

35 USC 103 Rejections:

Claims 8-10 and 14-19 are rejected under 35 USC 103(a) as being unpatentable over Walker (US Patent No. 6,163,771), Slater (US Patent No. 6,098,093) and Hurst (2003-0226030). Claims 11 and 13 are rejected under 35 USC 103(a) as being unpatentable over Walker, Slater, Hurst and in view of Kuroda (US Patent No. 6,470,448).

Claims 6, 12, 20, 21, 23-25, 29 and 31 are rejected under 35 USC 103(a) as being unpatentable over Walker, Slater, Hurst, Kuroda and Husemann (US Publication No. 2001/0037264).

The independent claim is 10, which is rejected as being obvious over Walker, Slater and Hurst. Walker is newly cited and newly relied upon.

The Office Action newly relies upon Walker FIG. 3B, items 360 and 361 and column 6, lines 15-39 and 61-67 for allegedly discussing the claimed key derivation. However, Walker

does not cure the deficiencies of Slater or Hurst, because Walker column 6, lines 15-39 discusses the 'The cardholder first inputs his PIN or biometric data to access a device (step 351)," which differs from the language of claim 10 requiring "***generating ... a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement ..., securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***."

In addition, Walker steps 360 and 361 discuss generating a single-use credit card number, where the "number is unique for the specified input variables set by the cardholder or by the device. It may also be unique to the specific date and time to avoid so-called 'replay' attacks for that card at that merchant with that exact purchase amount." Walker column 6, lines 61-67 also discusses 'the single-use credit card number is generated by the device cryptoprocessor 205, using a private key 601 stored in the device memory 104 (preferably the ROM 204).' However, the language of claim 1 does not generate a single-use credit card number, and the single-use credit card number fails to expressly or implicitly disclose a key derived based upon both a mobile device parameter and an input mobile device parameter and the key used to secure a first view of an agreement. In other words, Walker's single-use credit card number is not used to secure an agreement. In addition, Walker discusses use of the PIN to access a device, but fails to disclose expressly or implicitly use of the PIN to generate a key for securing agreement data.

In addition, Walker's single-use credit card number generated using a private key cannot correspond to the claimed "first view of the agreement ..." because the language of claim 10 requires the "first view of the agreement" to be secured by "***generating ... a first mobile device parameter derived from a stored mobile device parameter ..., securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***." In other words, Walker's single-use credit card number is not secured by a key, but is generated by a private key 601.

In addition, Slater discusses DES and Hurst discusses deriving a key based upon a stored secret key and a stored memory device identifier (column 8, claim 7 and paragraphs 46-

47). Slater's DES differs from the claimed symmetric agreement verification protocol, because Slater column 8, lines 14-16 discusses a conventional DES in which the financial institution 22 holds the decryption key. However, the language of amended claim 10 requires "***generating ... a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement ..., securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***."

In addition, the language of claim 10 requires "***the first view of the agreement not including the first and second mobile device parameters***." For the claimed mobile device parameters, the Office Action relies upon Slater column 7, lines 66-67 and column 8, lines 1-28, and column 9, lines 809, however, Slater only discusses using the PIN 'by a cardholder to identify themselves to their bank to authorize on-line ATM/POS transaction,' and Slater column 8, lines 17-21 expressly discuss 'Card reader device 64 forwards the encrypted card information 39 and security information 40 [i.e., PIN] (column 7, lines 60-63) to computer 50, ...' So Slater expressly discusses encrypting both the card information 39 and security information 40 and transmitting the encrypted card information 39 and security information 40.

Therefore, Slater fails to expressly or implicitly disclose to one skilled in the art to be modified to provide the claimed "***generating ... a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement ..., securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device,*** and transmitting the first view of the agreement to the second party, ***the first view of the agreement not including the first and second mobile device parameters***." In other words, Slater's card information 39 and security information 40 (PIN) cannot correspond to both the claimed "***first view of the agreement***" and the claimed "***a first mobile device parameter derived from a stored mobile device parameter ... and ... a second input mobile device parameter*** ... transmitting the first view of the agreement to the second party, ***the first view of the agreement not including the first and second mobile device parameters***," since Slater expressly discusses encrypting both the card information 39 and security information 40 and transmitting the encrypted card information 39 and security

information 40. So in Slater the card information 39 and security information 40 would be part of the transmitted agreement.

Further, in Slater, both the card information 39 and the security information 40 are input via the card 44, whereas the language of the claims only provides for one of the mobile device parameters to be input.

Further, for key derivation, the Office Action relies upon Hurst, however, Hurst paragraph 47 and Hurst claim 7, as illustrated by FIG. 4, discuss deriving a key from a hidden secret key 424 and a memory device identifier 426, both of which are stored. In other words, Hurst discusses unlocking the SSC 420 of the MultiMedia Card (MMC) based upon a stored hidden key 424 and stored MMC ID 426, so Hurst is silent on ***an input mobile device parameter***. However, the language of amended claim 10 requires "***generating ... a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement ..., securing the first view of the agreement based upon a key derived from both a the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device,*** and transmitting the first view of the agreement to the second party, ***the first view of the agreement not including the first and second mobile device parameters***."

Further, Hurst paragraph 47 and claim 7, as illustrated by FIG. 4, expressly discuss the derived key based upon both the key 424 and the MMC ID 426 are used to unlock the Secured Content Container (SCC) 420, which is located on the MultiMedia Card (MMC). In other words, Hurst does not use the derived key to provide the claimed "***securing the first view of the agreement based upon a key derived from both a the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***."

Further, Hurst is silent on and fails to suggest, expressly or implicitly, conducting an agreement between parties using a mobile device, since Hurst only discusses using its derived key for activating protected content on a portable memory device of the mobile terminal (Abstract, FIG. 4, paragraphs 46-47).

Further, Walker, Slater and Hurst are silent on the claimed "***trusted third party server*** ... ***verifying conditions of the agreement*** ... based upon ***... deriving the key based upon the first and second mobile device parameters for the secured first view and using the first and second merchant device parameters for the secured second view***," because as acknowledged by the Office Action, Slater is silent on the claimed key derivation, Hurst does not conduct an agreement between parties involving the mobile terminal, and for the reasons discussed above Walker does not derive a key according to the language of claim 10.

In other words, the Office Action alleges that Slater discusses a first and a second parameter, namely the card information 39 and the security information 40, which are encrypted by a key and transmitted, and that Hurst discusses deriving a key from two parameters, which can be combined with Slater for encrypting Slater's first and second parameters. The Office Action page 8, last line, provides 'Thus, substituting the encryption method taught by Slater with the method Hurst is obvious. The simple substitution of one known element for another producing a predictable results render the claim obvious.' However, a simple substitution of Hurst's encryption for Slater's encryption would not achieve the language of claim 10 without further modification, because the language of claim 10 requires "***generating ... a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement ..., securing the first view of the agreement based upon a key derived from both a the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***" and "transmitting the first view of the agreement to the second party, ***the first view of the agreement not including the first and second mobile device parameters***." In other words, it would not be a simple substitution between Hurst and Slater, because the combination of Slater and Hurst teaches away from the present invention or would result in a very weak encryption method (unsecure), such that providing a very strong encryption method according to the language of claim 10 could not be predictable.

Because, if as the examiner alleges one could use Hurst to derive a key from first and second parameters of Slater, namely the card information 39 and the security information 40 [i.e., PIN], and then use that key to encrypt and transmit both the encrypted first and second parameters, namely transmit the encrypted card information 39 and the security information 40 [i.e., PIN], aside from the fact that the language of the claims only requires using the derived key

for "***securing the first view of the agreement*** ... ***the first view of the agreement not including the first and second mobile device parameters***," a problem would be that the first and second parameters would be encrypted with a key derived from the first and second parameters. It is submitted this could be a very weak encryption method (might be unsecure), because the derived key is also used to encrypt itself (i.e., the first and second parameters) which can make successful attacks faster than a brute force attack (trying all possible keys), since the plaintext (first and second parameters) is also present in the key that is used to encrypt it.

Thus, it is submitted that one skilled in the art would not use the Hurst method to derive a key from first and second parameters and then encrypt the first and second parameters with the derived key (combined Slater and Hurst), because this would result to very weak security. In other words, Slater's card information 39 and security information 40 (PIN) cannot correspond to both the claimed "***first view of the agreement***" and the claimed "***a first mobile device parameter derived from a stored mobile device parameter ... and ... a second input mobile device parameter***," since the language of amended claim 10 requires "***securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device*** ... and transmitting the first view of the agreement to the second party, ***the first view of the agreement not including the first and second mobile device parameters***."

A prima facie case of obviousness based upon Walker, Slater and Hurst cannot be established, because nothing has been cited or found that Walker, Hurst or Slater expressly or implicitly disclose to one skilled in the art to combine Walker, Hurst and Slater and then further modify Walker's use of a PIN to access a device and a single-use credit card number generated based upon a key, but the key is not used to secure agreement data or derived according to the language of claim 10, with Hurst's key derivation for unlocking the SCC 420 to provide the claimed "***input personal identifying information of the first party as a second input mobile device parameter***" when Hurst is silent on an input parameter; and then even further modify Hurst's mobile terminal to provide the claimed conducting an agreement between parties; and even further modify Slater's discussion of using the PIN 'by a cardholder to identify themselves to their bank to authorize on-line ATM/POS transaction,' and Slater's column 8, lines 17-21

discussion of 'Card reader device 64 forwards the encrypted card information 39 and security information 40 [i.e., PIN] to computer 50, ...', to provide the claimed "***generating ... a first mobile device parameter derived from a stored mobile device parameter and generating a first view of the agreement ..., securing the first view of the agreement based upon a key derived from both ~~a~~ the generated first mobile device parameter ~~stored in the mobile device~~ and input personal identifying information of the first party as a second input mobile device parameter input to the consumer mobile ~~device~~device***," in combination with other claimed features, namely "transmitting the first view of the agreement to the second party, ***the first view of the agreement not including the first and second mobile device parameter***" and "***open and non-secure wireless network***," and "***trusted third party server verifying conditions of the agreement ... based upon ... deriving the key based upon the first and second mobile device parameters for the secured first view and using the first and second merchant device parameters for the secured second view***," and "wherein ~~***only***~~ ***the STS exclusively stores ... the second input mobile device parameter***," and seen the following benefits:

A benefit of the embodiments is to substantially reduce the risk of unauthorized derivation of the key, because only one of the parameters based upon which the key is derived is stored in the mobile device and the other second parameter is ***input***, namely "***input personal identifying information of the first party as a second input mobile device parameter*** input to the consumer mobile device." So even if the mobile device is lost or used by other than the user, an agreement and/or the key cannot be conducted/derived without the "***second input mobile device parameter***." And even if the first view is intercepted, it is very difficult to reverse engineer the first and second parameters, because of "***the first view of the agreement not including the first and second mobile device parameters***."

Another benefit is that a secure channel in wireless communication environment may or may not be used according to application criteria, for example, if desired to avoid pre-arrangement, or in case of SSL, speed wireless communication and/or not require key distribution, management and storage at wireless mobile device, which might not practical from a usability perspective (see paragraphs 239 and 478-479 of the present application).

Withdrawal of the rejection of independent claim 10 and allowance of claim 10 is requested.

Dependent claims recite patentably distinguishing features of their own or are at least patentably distinguishing due to their dependencies from the independent claim 10.

It is believed, the claims are now in condition for allowance, which is respectfully requested.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,
STAAS & HALSEY LLP

Date: June 16, 2009

By: /Mehdi D. Sheikerz/
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501